Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended) A computer-readable medium having computer-executable instructions for performing a process, the process comprising:

monitoring access by a host servers of digital tracking components residing on a remote client during digital communication between the remote client and the host servers with a color coded visual alert; and

providing an audible alert to the remote client when ~~the~~ one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the particular host server;

wherein the color coded visual alert is a graphical display that displays a safe color when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server and a warning color when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.

Claim 2 (original) The computer-readable medium for performing a process of claim 1, wherein the information is information about the remote client that is associated with other host servers.

Claim 3 (original) The computer-readable medium for performing a process of claim 1, wherein the information that is not associated with the host server making the request contains confidential information.

Claims 4-5 (canceled).

Claim 6 (original) The computer-readable medium for performing a process of claim 1, wherein the remote client communicates with the host server via a networked connection.

Claim 7 (original) The computer-readable medium for performing a process of claim 6, wherein the networked connection is a World Wide Web Internet connection.

Claim 8 (original) The computer-readable medium for performing a process of claim 7, wherein the method operates within a World Wide Web browser.

Claim 9 (original) The computer-readable medium for performing a process of claim 8, wherein the digital tracking component is a cookie that is used by the World Wide Web browser.

Claim 10 (original) The computer-readable medium for performing a process of claim 1, further comprising displaying in symbolic format the digital tracking components that the remote client has residing in a memory location.

Claim 11 (currently amended) In a computer system having a connection between a remote client and a host server, a method of protecting the remote client from digital intrusions, the method comprising:

monitoring access by host servers of digital tracking components of the remote client with a color coded visual alert; ~~and~~

providing an audible alert to the remote client when a request of a particular digital tracking component by a particular host server is made if the particular host server is not associated with the requested digital tracking component;

displaying a safe color with the color coded alert when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server; and

displaying a warning color with the color coded alert when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.

Claim 12 (original) The method of claim 11, wherein the remote client includes a graphical user interface including a display and a user interface selection device for providing the alerts.

Claims 13-14 (canceled).

Claim 15 (original) The method of claim 14, wherein the connection between the remote client and the host server is a World Wide Web Internet connection.

Claim 16 (currently amended) A computer security system for preventing host servers from taking inappropriate self-contained packets of information residing on a remote client, the system comprising:

a monitor module that monitors requests by the host servers of the self-contained packets of information residing on a remote client during digital communication between the remote client and the host server with a color coded visual alert; and

a notify module that provides an audible notification to the remote client when a particular host server requests one or more of the self-contained packets of information that contains information that is not associated with the particular host server;

wherein the color coded visual alert is a graphical display that displays a safe color when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server and a warning color when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.

Claims 17-18 (canceled).

Claim 19 (original) The computer security system of claim 16, wherein the monitor and notify modules operate within a World Wide Web browser and the self-contained packets of information are cookies.

Claim 20 (original) The computer security system of claim 19, wherein the notify module displays in symbolic format the cookies that the remote client has residing in a memory location.

Claim 21 (currently amended) A method of transacting data between a first and a second computer, comprising:

monitoring data requests from the first computer by the second computer with a color coded visual alert;

determining whether the second computer should have access to the data requested; ~~and~~

preventing the second computer from accessing the data if it is determined that the second computer should not have access to the data;

displaying a safe color with the color coded alert when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server; and

displaying a warning color with the color coded alert and sending an audible alert when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.

Claim 22 (original) The method of claim 21, wherein the transaction of data occurs over the Internet.

Claim 23 (original) The method of claim 22, wherein the data is a digital tracking component.

Claim 24 (original) The method of claim 23, wherein the transaction of data occurs within a World Wide Web browser environment and the digital tracking component is a cookie.

Claim 25 (currently amended) A computer-readable medium having computer-executable instructions for performing a process for transacting data between a first and a second computer, the process comprising:

monitoring data requests from the first computer by the second computer with a color coded graphical alert;

determining whether the second computer should have access to the data requested; ~~and~~

preventing the second computer from accessing the data if it is determined that the second computer should not have access to the data;

displaying a safe color with the color coded graphical alert when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server; and

displaying a warning color with the color coded graphical alert and sending an audible alert when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.

Claim 26 (original) The computer-readable medium for performing a process of claim 25, wherein the transaction of data occurs over the Internet.

Claim 27 (original) The computer-readable medium for performing a process of claim 26, wherein the data is a digital tracking component.

Claim 28 (currently amended) The computer-readable medium for performing a process of claim 27, wherein the transaction of data occurs within a World Wide Web browser environment and the digital tracking component is a cookie.

Claim 29 (currently amended) A computer security system for preventing inappropriate transaction of data between a first and a second computer, the system comprising:

a monitor module that monitors data requests from the first computer by the second computer with a color coded visual alert;

an access module that determines whether the second computer should have access to the data requested; ~~and~~

a prevent module that sends an audible alert to the first computer and prevents the second computer from accessing the data if it is determined that the second computer should not have access to the data;

wherein the color coded visual alert is a graphical display that displays a safe color when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server and a warning color when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.

Claim 30 (original) The computer security system of claim 29, wherein the transaction of data occurs over the Internet.

Claim 31 (currently amended) The computer security system of claim 30, wherein the data is a digital tracking component.

Claim 32 (original) The computer security system of claim 31, wherein the transaction of data occurs within a World Wide Web browser environment and the digital tracking component is a cookie.